SECURITY MEASURES

IW 130

OPR: Captain Gerry Eisert

DESCRIPTION: This lesson discusses the Information Warfare pillar, Security Measures.

METHODOLOGY: Informal Lecture/1.0 Hour

COGNITIVE OBJECTIVE: The objective of this lesson is for each student to comprehend the Security Measures of Information Warfare.

COGNITIVE SAMPLES OF BEHAVIOR:

1. Identify the major components of IW Security Measures.

2. Identify the elements with fall under Information Security/Assurance.

3. Explain how Security Measures support Information Warfare.

AFFECTIVE OBJECTIVE: The objective of this lesson plan is for each student to respond positively to the security measures of Information Warfare.

SAMPLES OF BEHAVIOR:

1. Effectively discuss how the components of IW Security Measures could enhance the warfighter's mission.

2. Positively participate in "real world" examples of IW Security Measures.

3. Effectively discuss how IW Security Measures could be used in peace, war and military operations other than war (MOOTW).

REQUIRED READINGS:

1. *Security and the Domestic Infrastructure, John H. Gibbons, Assistant to the President for Science and Technology, Instructional Circular page 130-H-1.*

2. *Threat to Corporate Computers Is Often Enemy Within, Peter H. Lewis, Instructional Circular pages 130-H-2 through 130-H-5.*

Security and the Domestic Infrastructure

The domestic infrastructure which underpins the economic life of our society increasingly depends on electronic networks for the flow of essential information. In sectors such as transportation, finance, energy, and telecommunications, computer networks have become indispensable in providing essential services that we take for granted. Air traffic data for the safe conduct of thousands of flights per day, financial transactions worth many millions of dollars daily, and control signals for operation of power distribution grids, railroads, pipelines, and the telephone system itself, all travel over electronic networks. Electronic networks have truly become the "nerves" of our infrastructure in yet another manifestation of the proliferation of information technology that characterizes the world of today.

How reliable are these networks? How can we ensure they are reliable enough? These pressing questions are not easily answered. Our critical infrastructure information networks face many reliability challenges, from natural disasters to human error, and from equipment failure to terrorists and computer hackers. From a technical standpoint, these are not different problems; they are different parts of the same problem. A systematic sector-by-sector analysis of threats and vulnerabilities, and a sustained system engineering process that emphasizes reliability are the technical ingredients of a successful approach to managing these risks.

As powerful a tool as technology can be, it is not the whole answer. Technology, and especially information technology, is best understood in its societal context. People represent both the strongest and the weakest links in the reliability chain. We should therefore not lose sight of the human element as we focus on the technical challenges of assuring infrastructure reliability. Instilling a culture of vigilance in the community responsible for the infrastructure is the most fundamental step in preventing reliability problems.

Deciding how much reliability we need for our infrastructure, against what threats, and at what cost are questions of public policy that will require the sustained consideration of stakeholders throughout society. This report seeks to promote a common understanding of the network reliability challenge in the technical and policy communities in private industry, public utilities, and government at all levels. The efforts of these diverse players, through the broad dialogue of democracy, will be necessary to effectively respond to this long-term challenge.

John H. Gibbons

Assistant to the President

for

Science and Technology

Ref: CYBERNATION: *The American Infrastructure in the Information Age:* A Technical Primer on Risks and Reliability

Threat to Corporate Computers Is Often Enemy Within

By PETER H. LEWIS

The computer supervisor at a Midwestern engine manufacturing company approached his bosses last month and made them an offer they could not refuse. Either they gave him a big raise immediately and agreed to a list of other job demands, or he would shut the company down, according to Erik Thompson, a computer security consultant who was called in to help the firm after the incident.

The employee, Thompson said, got his raise, and yet another company discovered what thousands of businesses have learned the hard way in recent years: Despite justifiable fears about rogue programmers attacking an organization's information systems over the Internet, the greatest threat to a company's data security probably works just down the hall.

"Nobody wants to think that the guy I work with may be a bad guy, my worst nightmare," said Charisse Castagnoli of Internet Security Services Inc., an Atlanta-based consulting company. "If you look at the statistics, though, about 70 percent to 80 percent of security breaches are internal."

According to an informal survey conducted by the Computer Security Institute, an association of corporate data-security officers, for the FBI's International Computer Crime Squad, computer attacks by insiders were more common last year than external, Internet-based attacks.

More than 87 percent of the corporate, financial, government and university information-security managers polled by the survey said disgruntled employees were the most likely cause of data security "incidents," ranging from sabotage, fraud and theft of proprietary information to unauthorized snooping in a colleague's e-mail or storing digital pornography on a company computer.

Several different dynamics are increasing the risk of insider fraud or sabotage, security officials said. Companies increasingly are relying on outside contractors for technical work, and giving those outsiders insider privileges, in part because of a shortage of programmers exacerbated by the work needed to fix "year 2000" programming flaws.

"The Y2K problem is causing a lack of programmers, and people are hiring anybody," said Michael Zboray, a vice president at The Gartner Group in Stamford, Conn.

"Companies are now doing Y2K development offshore, sending work to Russia and India, and they haven't a clue as to what's coming back. They don't do background checks. What we're hearing is an undercurrent of back doors being programmed in."

According to the Computer Security Institute, companies employ on average one computer-security administrator for every 1,000 users of the computer system. The

budget for computer security, traditionally 1 percent to 3 percent of the total information-technology budgets for many corporations, is expected to rise to 3 percent to 5 percent this year, the institute said.

But, as with the case of the automotive-engine manufacturer, most companies are fearful of adverse publicity and never report internal security breaches, even the most severe ones, to law-enforcement agencies, security analysts contend.

"Most firms would rather go public with the news that their chief executive officer was an active alcoholic than the news that there was an insider security problem," said William Malik, a vice president and research director for Gartner Group.

One notable exception occurred last month when a former computer network administrator for a government subcontractor was arraigned in federal court in New Jersey, charged with having destroyed critical company data in 1996 using a software "logic bomb" that detonated three weeks after he was dismissed from his job.

The logic bomb erased all of the engineering programs and files at Omega Engineering Inc. of Bridgeport, N.J. Backup tapes were stolen as well, and losses from the sabotage could eventually cost the company more than $10 million, U.S. Secret Service investigators said.

Speaking to a data-security conference last month, Dan Nielsen, a special agent with the FBI's newly renamed National Infrastructure Protection Agency, said insider attacks are rarely reported, and thus the agency has no reliable estimate of the dollar losses sustained from them. But the tally for the relatively few attacks that were reported in 1996 was $100 million, according to the Computer Security Institute/FBI survey.

Early responses from the 1997 year-end survey indicate a 30 percent rise in reported losses in the past 12 months, said Richard Power, president of the Computer Security Institute. And it appears the percentage of companies reporting computer-security incidents in 1997 will also rise sharply, to more than 60 percent, he said.

Half of the 563 information security professionals responding to the 1996 survey said their organizations had sustained the unauthorized use of systems last year, and among those, insider attacks were reported to be more common than external attacks.

The 249 organizations that were able to quantify the losses from all computer attacks reported losses totaling $100 million. The Computer Security Institute is now compiling results from the 1997 survey.

Instead of going to the legal authorities, victims of inside attacks typically go to the technical authorities. There is a growing industry of computer-security consultants and disaster-recovery experts.

Thompson, the computer-security consultant who was called in last week to help rescue the engine manufacturing, said of the employee: "He was the only one who could run the software that made the manufacturing hardware work. They couldn't fire him,

because firing him shuts down the assembly line, and by the time they get someone else in there to replace him, they are out of business."

Legends abound in the computer world about programmers and system administrators who booby-trap the systems they create, using such potential software weapons as logic bombs, back doors and encryption as leverage in case they are dismissed or not paid.

"It's very common," Thompson said. "We deal with three or four cases of disgruntled employees a day, typically encrypted files. Word-processing files, spreadsheets, accounting, payroll, engineering diagrams -- it depends on what's critical to the business."

Encryption, formerly the province of military and government spies, has now become a tool embedded into standard commercial software. It allows files to be scrambled so that only the person with the proper password can unlock and read the file. It is common for employees to encrypt a file and forget the password, but some employees encrypt files for malicious reasons.

"Lawyers are the worst," Thompson added, saying that they were prone to anger their secretaries. "The secretary is the one who runs the business. She encrypts the case files, and says, 'To hell with you, I'm not going to give you the passwords.' The lawyer has to be in court the next day. It happens several times a week."

If a disgruntled employee is a potential nightmare, the mother of all nightmares is a disgruntled system administrator, or sysad. The sysad typically has access not only to sensitive company files, but also to the security systems that guard them from unauthorized users within and outside the company.

"The most powerful person in your company is the sysad," said Peter Shipley of Berkeley, Calif., one of the United States' top computer-security experts.

But he said that the system administrators are often underpaid and underappreciated. "The attitude is, if things are working flawlessly, you're obviously not doing any work, and if things are failing, obviously you're not doing your job. Unfortunately that's the way it works," Shipley said.

To be sure, tens of thousands of system administrators around the country have a reverential attitude toward protecting the data in their care, and so far only a relative handful have used their power to intimidate or gain revenge on a company. But security analysts say any organization that gives one person control over critical "choke points," like computer networks, is making a grave mistake.

Katherine Fithen, manager of operations for the Computer Emergency Response Team, a quasi-government agency in Pittsburgh that is responsible for tracking and responding to security violations at networked computer sites, said her group seldom hears from companies whose systems have been attacked from within.

But, she added, CERT has received several queries recently from companies that were about to dismiss their system administrators, asking how they could protect themselves,

just in case.

"The sysadmin knows the inside of the system, knows how the networks are configured, how the trust mechanisms between machines work, and they have the best understanding of how to do damage," she said.

Last year, companies in the United States spent hundreds of millions of dollars buying and installing network-security tools, including network firewalls, which are combinations of computer hardware and software intended to keep unauthorized visitors from penetrating a company's internal network and gaining access to sensitive information.

But if the attacker already has authorization, Shipley noted, firewalls can fail to protect a system even if they function perfectly. Companies that install the computer equivalent of thick steel doors to keep out intruders may have only screen doors internally, he said. And programmers often know how to tunnel through the firewall, creating fictitious user accounts, or leaving open a "back door" into the system to allow outside access.

"It starts innocently enough," said Castagnoli, of Internet Security. "You're going to work from home, you're an administrator, you need remote access. Where it goes over the line is when people start putting in protections for themselves, to cover their tracks. Then there's the what-if scenario: If something happens to me, I'm going to get back at them. Now we're in the category of revenge."

"There was a relatively recent case on Wall Street, where a sysad at one of the financial houses was fired," she said. "He had remote home access, and came back in from home and deleted a number of sensitive files."

And last month, the complete payroll data base of Pixar Inc., a computer firm best known for its work in creating special effects for movies, was distributed to all employees via an e-mail message purportedly sent by the company's chairman, Steve Jobs. Jobs denied sending the list, and company officials said they suspected that a disgruntled employee was responsible.

Last April, a temporary employee in New York was charged with breaking into the computer system of Forbes Inc., the publisher of Forbes magazine, and causing a system crash that left hundreds of employees unable to use their computers and cost the company more than $100,000.

While incidents of both internal and external computer crimes are on the rise, some see a positive sign in the fact that more cases of computer attacks are being reported. "The growing acceptance that there is a widespread problem has probably led other people to go ahead and admit to incidents," said Power of the Computer Security Institute. And the FBI said more companies are coming forward to share information about internal security problems. Date: Monday, March 2, 1998